Advancing the Business of Technology

Frank E. Moss
Deputy Assistant Secretary
Passport Services
U.S. Department of State
Room 6811
Washington, DC 20520

Elaine Dezenski
Acting Assistant Secretary
Border and Transportation Security Policy
U.S. Department of Homeland Security
Washington, DC 20528

January 30, 2006

VIA EMAIL: mossfe@state.gov, elaine.dezenski@dhs.gov

RE: Privacy and Security Concerns with the use of EPCglobal UHF Generation 2 technology in the Western Hemisphere Travel Initiative Card Program.

Dear Acting Assistant Secretary Dezenski and Deputy Assistant Secretary Moss:

The undersigned companies are expressing their thanks for the opportunity to discuss the Western Hemisphere Travel Initiative (WHTI) with you, an important program aimed at securing our nation's land borders. We share the goals of both the Department of State (DoS) and Department of Homeland Security (DHS): to quickly, securely and effectively process travelers across the U.S. land boarders without impeding commerce with our most important trading partners. However, we also have some concerns with the direction the program is taking regarding the consideration of a possible technology solution. Our concerns rest primarily in the areas of privacy of the citizen using the document and the security of our nation.

AeA is the nation's largest high-tech trade association, representing more than 3,000 companies with 1.8 million employees across the United States. AeA's member companies span the high-technology spectrum, from software, semiconductors, medical devices and computers to Internet technology, advanced electronics and telecommunications systems and services. AeA has been the accepted voice of the U.S. technology community since 1943. For more information, we invite you to visit our website at www.aeanet.org/RFID.

As a part of The Intelligence Reform and Terrorism Prevention Act of 2004, the DoS and DHS are directed to develop and implement a plan to require U.S. citizens and foreign nationals to present a passport or a secure document when entering the United States. The Western Hemisphere Travel Initiative (WHTI) will require all U.S. citizens, citizens of the British Overseas Territory of Bermuda and citizens of Canada and Mexico to have either a passport of other accepted secure document that establishes the holder's identity and nationality to enter the U.S. It is our understanding the State Department expects that acceptable documents must establish the citizenship and identity of the bearer through electronic data verification and will include significant security features. It is our belief that serious consideration must be given to creating a travel document that incorporates these electronic security capabilities using a smart chip, which accomplishes the security requirements of identification and entry and exit tracking in the most secure and efficient manner.

It is our understanding that the WHTI program is contemplating use of the EPCglobal UHF Generation 2 (Gen 2) technology as a possible technology solution. We have grave concerns over this selection, primarily in the areas of privacy and security.

Privacy and Security Concerns with the EPCglobal Generation 2 Standard
As you may know, EPCglobal was founded as principally a member-driven organization by leading retail, consumer product goods manufacturers, and technology companies to develop a standard for supply chain logistics. UHF technology is considered a good fit for identifying cases and pallets of goods moving through the retail supply chain for the purposes of highly efficient and rapid inventory tracking. The EPCglobal Generation 2 standard was engineered specifically for high performance in conditions encountered in supply chains, including in warehouses, distribution centers, and retail locations. The Gen 2 standard was never designed for use in identifying people and included no security or privacy mechanisms designed for this purpose. *As such, solutions contemplating the use of EPCglobal Gen 2 standards are inappropriate for personal identification applications, which demand far higher security, including protection of individual privacy.*

With regard to privacy, Generation 2 technology is designed for maximum read range under different conditions. Utilizing EPCglobal UHF Generation 2 technology would thus perversely maximize the possibility, raised by numerous privacy groups, of an illicit actor "tracking" a person at very long ranges, on the order of 30 feet, or more. While UHF Gen 2 does allow for a random temporary ID, like the RUID now being built into the US ePassport, the strength of the cryptography covering the actual user ID is very weak.

Furthermore, Generation 2 does not offer security features demanded by personal ID applications. Gen 2 lacks any form of anti-counterfeiting protection, making it highly susceptible to forgery. A potential illicit hacker could very easily read (again, from a distance) the unique ID contained in a proposed Gen 2-based land border crossing card, and easily create a duplicate. The scenario can be imagined where a potential terrorist surreptitiously skims the EPC number information from the unsecured WHTI Gen 2 card and then easily creates a duplicate card which could then be used in one of the proposed "fast lanes." All the potential terrorist need do is be sure that the holder of the fake card resembles the holder of the true WHTI card in order to pass a cursory visual inspection by a border-crossing guard.

The companies signing this letter strongly urge you to re-consider the use of Generation 2 consumer goods supply chain technology for use in secure personal identification. The use of Gen 2 in the WHTI application would potentially threaten individual U.S. citizen privacy and potentially undermine critical homeland security border control programs and effectiveness.

Protecting American Security: Using the Right Tools for the Job.
Instead, we urge you to evaluate proven solutions that provide enhanced anti-counterfeiting capabilities and that preserve individual privacy. For the land border application described, contactless smart card-based integrated circuit chip technology solutions designed around the ISO 14443 standard would provide a secure identification transaction while not substantially adding to individual border crossing times. This solution is tremendously cost effective and does not add substantial cost to individual credentials. A minimal additional investment in the individual credential, adding security and privacy features, would still allow the Departments to employ a "database pointer" system. The only difference would be that, instead of a "portal" at the proposed "yellow line" waiting area at a border crossing point, travelers would instead present their cards to a parking garage style reader placed next to the vehicle. Transaction times would be extremely comparable, at minimal additional cost per secure credential. Smart card capabilities to randomize the temporary ID used by the reader and credential would furthermore address concerns about "tracking" of a unique ID. Smart card technology would also provide an anti-counterfeiting measure currently not incorporated into other technologies, as well as anti-collision technology which would create the ability to deal with multiple cards at one time.

While this recommendation would turn what is now a "vicinity" card into "proximity" card, it would also enable the Department of State and the Department of Homeland Security to ensure consistency with the ICAO standards currently used in the U.S. passport. This would also serve cross-agency compatibility, as it would allow for the same issuance equipment and reader infrastructure to create and read both the ePassport and the WHTI card. In fact, the same Basic Access Control mechanism used on the ePassport could be used on the WHTI card, eliminating the need for a foil sleeve, something that is certain to be lost. If the same ICAO data format is adopted to that of the proposed ePassport implementation, the exact same ICAO PKI system can be utilized to verify the Issuer's Digital Signature, and hence integrity of the WHTI's credential data. No other cryptographic system would be needed, and by carrying the credential data, the WHTI card can be read and verified off-line from any database making a more robust, faster and less expensive implementation.

We look forward to working with you to address these issues in the next few weeks. It is critical to this program that we be able to present our concerns directly to your colleagues at the Department of Homeland Security. Our industry looks forward to working with both DoS and DHS to make the WHTI as secure and efficient as possible. We will be following up with both your offices by the end of the week to arrange a meeting when it is convenient for the both of you to discuss best security practices for the WHTI card program. In the meantime, if you have any questions, please do not hesitate to contact AeA's Counsel and Director of Technology Policy, Marc-Anthony Signorino, at msignorino@aeanet.org or 202/682-4428.

Sincerely,

AeA
Anteon International Corporation
Axalto Inc
Gemplus Corporation
Giesecke & Devrient Cardtech, Inc.
Infineon Technologies North America Corp.
Oberthur Card Systems of America
Philips Electronics North America
Texas Instruments, Inc.